Calamu™ | cimplifi™

Calamu Protect™

Make Your Data Unhackable

using data-first security

Click to watch video:

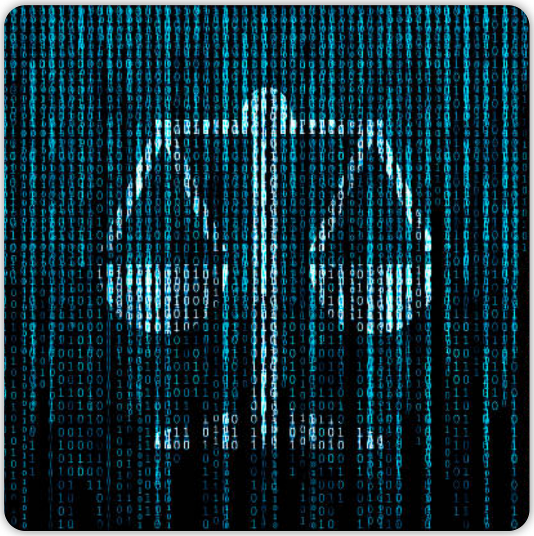
For the legal sector ransomware attacks and data theft is surging.

Common data security and protection solutions like encryption and backups alone do not solve the underlying cause of why cyber attackers can do so much damage. A data breach doesn't need to be a disastrous event.

75% of companies impacted by ransomware were running up-to-date endpoint protection[1]

22 days was the average cost in downtime from a ransomware attack[2]

400% increase in the number of ransomware attacks over the last year[3]



Despite existing solutions, the problem is getting worse!

Legal and professional services have become a constant target for ransomware gangs and other cyber criminals, and represent nearly a quarter of all ransomware victims in the U.S. The industry has put more emphasis on cybersecurity in recent years, typically using some form of encryption or data backups, but catastrophic data breaches continue to make headlines. Cyber attackers are using new tactics to gain access to sensitive data, and leaning more heavily on extortion as a way to ensure they profit from stolen files. The unfortunate reality is that extortion works – legal organizations work with highly sensitive information that isn't easily replaced, and when such data is published or exposed the effects are devastating. Even if the firm keeps a pristine backup copy of their data on a completely isolated server, the damage will have already been done. Recent events have proven that backups, encryption, and anti-virus alone are not enough to ensure data is truly protected, and the cost of remediation is typically in the hundreds of thousands to millions of dollars.

Sources: [1]Sophos | [2] Cybersecurity Ventures | [3]FBI

Unstructured data at-rest poses an especially high risk.

For most legal organizations and law firms, unstructured data sitting at-rest represents over 80% of the total data under their control. Client identities and payment information, confidential legal briefs, digital evidence, contracts, hearing records, and even private memos all create an undeniable target for hackers and ransomware attackers, and a significant data governance challenge. If an attacker gains access to these types of data they can do irreparable harm to the organization, causing expensive downtime and jeopardizing customer and client relationships.

Key challenges facing legal service providers in data security:

- Legal data volumes grow year-over-year and require long term retention
- Data backups are just as vulnerable as all other stored data and can no longer be relied on as a ransomware recovery mechanism
- High amounts of unstructured data files are difficult to manage and protect
- Third party platform vulnerabilities outside of the organization's control such as consultants, vendors, and contractors can expose data
- Many clients require cybersecurity audits, and firms need to prove data is protected
- Regulatory requirements such as GDPR and CPRA mandate client and customer data be protected

Calamu Protect™ at-a-glance:

Calamu Protect is a scalable, automated data-first security platform that enables you to effectively absorb ransomware attacks or any other data breach, by protecting data in a way encryption and backups cannot. Data protected using Calamu is highly resilient and becomes valueless to cyber attackers by eliminating all data sensitivity. The data is able to withstand any breach and remains immediately available to authenticated users and applications, but cyber attackers get only valueless Digital Sludge™.

Able to Withstand Any Data Breach

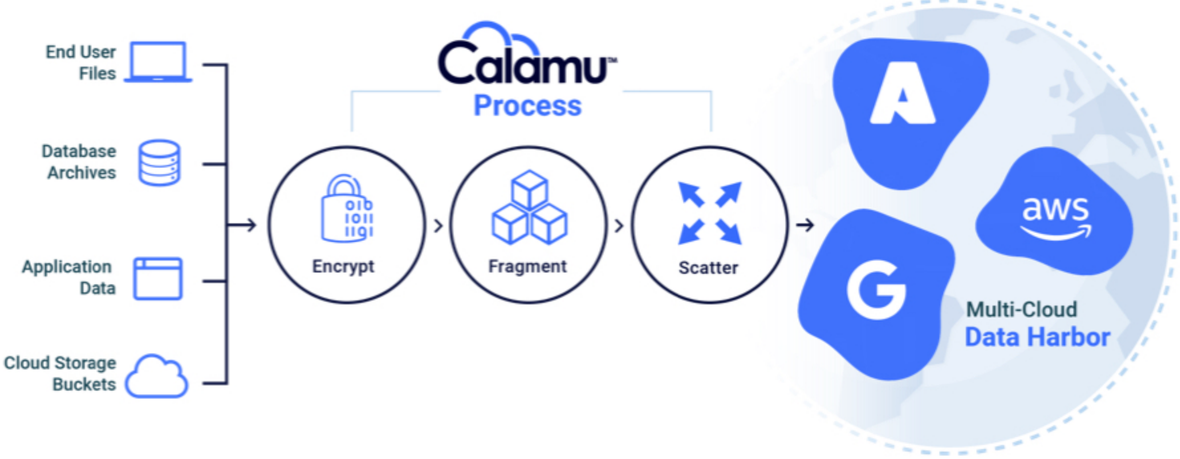
Attackers Get Digital Sludge

Eliminates Downtime

How it works:

Calamu Protect forms a **safe data harbor**, a virtual environment that is immune to the effects of ransomware or a data breach. Data processed using Calamu Protect is automatically encrypted, fragmented, re-encrypted individually, and scattered it to multiple storage locations that are physically separated. Once processed, sensitive data is automatically removed from source, ensuring that ransomware can't do any damage on the local machine or in the cloud. This provides users with a proactive approach that thwarts theft, exfiltration, and extortion tactics even in the event of a breach.

1. Calamu Protect encrypts and fragments the data which is then scattered across multiple storage locations that are physically separated.
2. The data is immune to a data breach, self-heals in the event of an attack, and helps compliance with many data privacy regulations such as GDPR.
3. The data remains immediately accessible to the rightful owners, even if a storage location is attacked or offline.



Benefits of data-first security:

- Protect any legal data from theft, manipulation, ransomware, or unauthorized access
- Secure data from applications, employee workstations, cloud storage buckets, and OneDrive
- Remove highly sensitive data files from unprotected devices with innovative protection
- Automatically self-heal from a data breach without using extensive backups, eliminating downtime
- Get rapid deployment and easy management
- Satisfy compliance or regulatory requirements for GDPR and others with ease

Works with major cloud providers and on-premise storage locations:

(V3)